

Contents

1	Introduction	1
1.1	Formal Verification Using Satisfiability Checking	1
1.2	Bounded Model Checking of Hybrid Systems	3
1.3	Solvers for Boolean Combinations of Numerical Constraints	5
1.3.1	Constraint Solving in a Nutshell	6
1.3.2	Contributions of the Thesis	9
1.3.3	Structure	12
1.3.4	Sources	12
2	Hybrid Dynamical Systems	15
2.1	Modeling Hybrid Systems with Hybrid Automata	16
2.2	Predicative Encodings of Hybrid Automata	23
2.2.1	A Basic Encoding Scheme	24
2.2.2	Hybridization of Continuous Dynamics	30
2.2.3	Encoding Flows Using Taylor Expansions	33
3	Extending DPLL for Pseudo-Boolean Constraints	37
3.1	The Logics	39
3.2	State of the Art in SAT Solving	40
3.2.1	Conversion into CNF	42
3.2.2	SAT Checkers for CNFs	45
3.3	Optimizing DPLL-Based Pseudo-Boolean Solvers	49
3.3.1	DPLL for Pseudo-Boolean Constraints	50
3.3.2	Generalization of Lazy Clause Evaluation	51
3.3.3	Learning in Presence of Pseudo-Boolean Constraints	53
3.4	Benchmark Results	55
3.5	Discussion	57
4	Integration of DPLL-SAT and Linear Programming	59
4.1	The Logics	60
4.2	Lazy Approach to SMT	62

4.3	SAT Modulo the Theory of Linear Arithmetic	63
4.3.1	Feasibility Check Using LP	65
4.3.2	Extractions of Explanations	65
4.3.3	Learning from Feasible LPs	68
4.3.4	Putting It All Together: a Sample Run	68
4.4	Optimizations for BMC	70
4.5	Benchmark Results	72
4.6	Discussion	74
5	Integration of DPLL and Interval Constraint Solving	81
5.1	The Logics	85
5.2	Algorithmic Basis	88
5.3	The ISAT Algorithm	90
5.3.1	Definitional Translation into Conjunctive Form	90
5.3.2	Split-and-Deduce Search	94
5.3.3	Arithmetic Deduction Rules	98
5.3.4	Correctness	104
5.3.5	Algorithmic Enhancements	109
5.3.6	Progress and Termination	112
5.4	Benchmark Results	114
5.4.1	Impact of Conflict-Driven Learning	114
5.4.2	Comparison to ABSOLVER	115
5.4.3	Comparison to HYSAT-1	119
5.5	Reachability Analysis with HYSAT-2: a Case Study	119
5.5.1	ETCS Model	120
5.5.2	Encoding into HySAT	124
5.5.3	Results	128
5.6	Discussion	130
6	Conclusion	133
6.1	Achievements	133
6.2	Perspectives	135
6.3	Final Thoughts	143
	Bibliography	145
	Index	159